Advanced Security 1 - CMPU4007
Week 1 - Introduction

Q1. Run the caesar cipher python code supplied (substitution), make it encrypt and decrypt using a key

```
def caesar(s, k, decrypt=False):
        if decrypt: k = 26 - k
    r = ""
    for i in s:
         if (ord(i) >= 65 and ord(i) <= 90):
                r += chr((ord(i) - 65 + k) % 26 + 65)
         elif (ord(i) >= 97 and ord(i) <= 122):
                r += chr((ord(i) - 97 + k) % 26 + 97)
         else:
                r += i
    return r

def encrypt(p, k):
        return caesar(p, k)

def decrypt(c, k):
        return caesar(c, k, True)
```

Q2. Run the rail fence cipher python code supplied (transposition), make it encrypt and decrypt using a key

```
def fence(p, k):
        fence = [[None] * len(p) for n in range(k)]
        rails = range(k - 1) + range(k - 1, 0, -1)
        for n, x in enumerate(p):
        fence[rails[n % len(rails)]][n] = x
        return [c for rail in fence for c in rail if c is not None]

def encrypt(p, k):
        return ''.join(fence(p, k))

def decrypt(c, k):
        rng = range(len(c))
        pos = fence(rng, k)
        return ''.join(c[pos.index(k)] for k in rng)
```

Links

https://repl.it/languages/python